DATENSCHUTZAKTUELL Professional
SEP | 2025
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

PERSONELLE ÄNDERUNGSMITTEILUNGEN: DIESE ASPEKTE SOLLTEN SIE PRÜFEN

Machen Sie Datenschutz zur Chefsache

Liebe Leserin, lieber Leser,

Datenschutz kann eine Erfolgsgeschichte sein, und zwar in jedem Unternehmen. Doch damit das klappt, braucht es nicht nur Sie als fähigen Datenschutzbeauftragten. Datenschutz muss auch gewollt sein und das vor allem ganz oben, bei der Unternehmensleitung.

Ist man dort noch nicht vom Datenschutz überzeugt, sollten Sie das nicht einfach hinnehmen. Sie können Datenschutz mit unkomplizierten Mitteln zur Chefsache machen. Heben Sie bei Besprechungen hervor, dass Datenschutz machbar ist und in erster Linie Vorteile bringt. Beispielsweise werden Risiken minimiert und Schaden wird vermieden.

Viele Grüße

Andreas Würtz,
Rechtsanwalt und Chefredakteur

Ihr Experte für Datenschutz
Andreas Würtz verfügt über mehr als 20 Jahre Berufserfahrung als Vollzeit-Datenschützer im Unternehmen. Er zeigt Ihnen, wie sich Datenschutz pragmatisch umsetzen lässt.

Inhalt

Zum neuen Onlinebereich!
www.privacyxperts.de/login

Expertensprechstunde:
https://t1p.de/andreas-wuertz

Bildnachweise:
Titel: Adobe Stock | InfiniteFlow
Seite 1: Adobe Stock | Thapana_Studio

Impressum

PRIVACYXPERTS

ein Unternehmensbereich des
VNR Verlags für die Deutsche Wirtschaft AG
Theodor-Heuss-Str. 2–4, 53095 Bonn
Telefon: 02 28 / 9 55 01 60
Fax: 02 28 / 3 69 64 80

ISSN: 1614 – 5674

Vorstand: Richard Rentrop, Bonn

V.i.S.d.P.: Michael Jodda
(Adresse s. oben)

Produktmanagement: Franziska Rohrbach, Bonn

Verantwortlicher Chefredakteur:
RA Andreas Würtz, Freiberg am Neckar

Design: Kreativ Konzept Agentur für Werbung, Bonn

Satz: Deinzer Grafik, Gartow

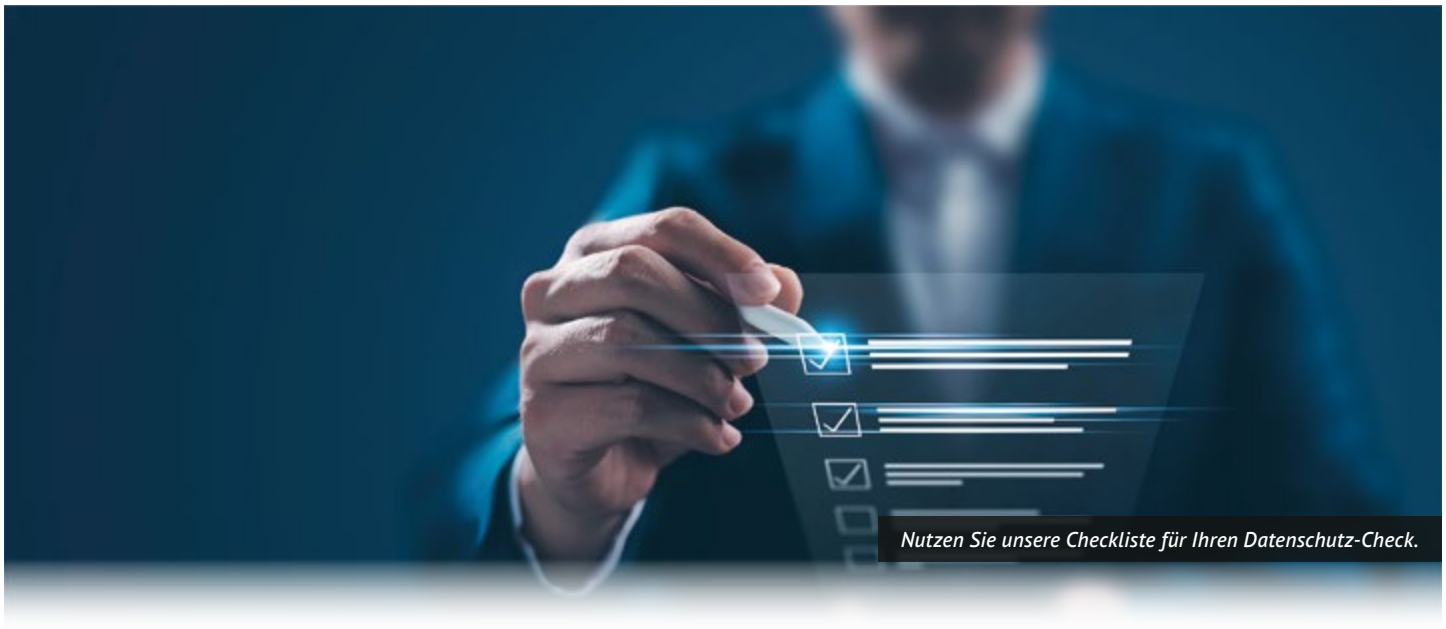
Druck: Warlich Druck Meckenheim GmbH, Am Hambuch 5, 53340 Meckenheim

Erscheinungsweise: 26-mal pro Jahr

E-Mail: kundendienst@privacyxperts.de

Internet: www.privacyxperts.de

(bei Rückfragen bitte Kundennummer angeben)



Nutzen Sie unsere Checkliste für Ihren Datenschutz-Check.

Gut aufgestellt im Datenschutz? Machen Sie den Check

Datenschutz ist kein Selbstzweck. Vielmehr schützt Ihr Unternehmen damit nicht nur Daten um des Schutzes willen. Es geht Ihrem Unternehmen in erster Linie darum, Gefahren und Risiken zu minimieren, um etwa Datenschutzverstöße zu vermeiden und keinen Ärger zu riskieren. Damit das so ist und bleibt, muss Ihr Unternehmen gut im Datenschutz aufgestellt sein. Machen Sie den Check!

Stellen Sie den Datenschutz auf den Prüfstand

Um zu beurteilen, wie es um die systematische Umsetzung des Datenschutzes im Unternehmen steht und inwieweit wichtige Aspekte der Datenschutz-Grundverordnung (DSGVO) umgesetzt sind, können Sie auf folgende Checkliste setzen. Stellen Sie fest, dass etwas nicht in Ordnung ist, sollten Sie die Initiative ergreifen und mit den zuständigen Kollegen oder der Unternehmensleitung sprechen. Schließlich besteht ernsthafter Handlungsbedarf.

CHECKLISTE: Bewertung des Datenschutzes im Unternehmen

Thema	Das ist besonders relevant	Erledigt?
Besteht eine solide Datenschutzorganisation?	› Hinterfragen Sie, wie der Datenschutz in Ihrem Unternehmen organisiert ist. Klären Sie insbesondere, inwieweit die vorhandene Organisation zu Struktur, Geschäftstätigkeit, Umfang der Verarbeitung personenbezogener Daten sowie Zahl und Qualifikation der Beschäftigten passt. › Seien Sie auch selbstkritisch im Hinblick auf Ihre Rolle und Ausstattung als Datenschutzbeauftragter. Sind Sie eher „Feigenblatt“ und können Sie Ihre Aufgaben nicht richtig wahrnehmen, ist das ein Problem, das das Unternehmen angehen muss.	☐ Ja ☐ Nein
Inwieweit ist ein Datenschutzmanagementsystem (DSMS) umgesetzt?	› Mit einem solchen System werden Strukturen und Prozesse etabliert, um den Datenschutzanforderungen gerecht zu werden. › Typisch sind das systematische Vorgehen und das Ziel, kontinuierlich die Datenschutzsituation zu verbessern. Dazu wird meist auf den PDCA-Kreislauf gesetzt, der für die Phasen Plan, Do, Check, Act steht, also Planen, Umsetzen, Überprüfen und Verbessern. › Im Fokus sind in erster Linie Regelungen zum Datenschutz, eine Organisation, relevante Prozesse sowie deren Umsetzung und fortlaufende Optimierung. › Ein solches Managementsystem ist an sich als „strukturiertes und systematisches Vorgehen“ zu verstehen. Gerade bei größeren Unternehmen kann der Einsatz einer entsprechenden Software zur Umsetzung des DSMS vieles erleichtern.	☐ Ja ☐ Nein
Wie werden Risiken mit Datenschutzbezug gemanagt?	› Risikomanagement ist in jedem Unternehmen eine unerlässliche Aufgabe, auch im Datenschutz. › Prüfen Sie, inwieweit Gefahren identifiziert, Risiken bewertet und passende Gegenmaßnahmen festgelegt werden. Dabei sollten Risikoanalysen systematisch ablaufen und klaren Regeln folgen. › Denken Sie nicht nur an Risiken mit Bezug zum Datenschutz bei der Verarbeitung personenbezogener Daten. Blicken Sie auch über den Tellerrand. So sind Mitarbeiter, die nicht über das nötige Know-how verfügen, genauso eine relevante Gefahr wie eine Tür zum Serverraum, die immer sperrangelweit offen steht.	☐ Ja ☐ Nein

CHECKLISTE: Bewertung des Datenschutzes im Unternehmen		
Ist ein vollständiges und aktuelles Verzeichnis von Verarbeitungstätigkeiten vorhanden?	› Das jeweilige Verzeichnis nach Art. 30 Abs. 1 oder 2 DSGVO ist nötig, um beispielsweise gegenüber der Datenschutzaufsichtsbehörde auskunftsfähig zu sein. Doch es ist auch wichtig für die Arbeit des Datenschutzbeauftragten. Es hilft dabei, den Überblick zu behalten und leichter die Verarbeitungen auszumachen, die einer besonderen Aufmerksamkeit bedürfen. › Achten Sie auf die Vollständigkeit und Aktualität der Angaben. Manchmal wird das Verzeichnis nur halbherzig geführt. Drängen Sie hier darauf, dass sich das schleunigst ändert. › Prüfen Sie auch, inwieweit Verarbeitungstätigkeiten ohne Technik (z. B. Verarbeitungen auf Messen, Listen) enthalten sind. Die werden gerne vergessen.	☐ Ja ☐ Nein
Sind für die Verarbeitungen personenbezogener Daten Risikoanalysen durchgeführt, Maßnahmen abgeleitet und umgesetzt?	› Grundsätzlich ist für jede Verarbeitung personenbezogener Daten eine Risikoanalyse erforderlich. Schließlich lassen sich nur so risikoangemessene technische bzw. organisatorische Maßnahmen auswählen. › Achten Sie darauf, dass Risikoanalysen nachvollziehbar und dokumentiert sind. Schließlich besteht auch diesbezüglich die Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO. › „Einmal Durchführen und dann vergessen“ ist nicht drin. Die Risiken müssen fortlaufend beobachtet und die Bewertung sowie Maßnahmen müssen ggf. angepasst werden.	☐ Ja ☐ Nein
Ist die Einhaltung der Grundsätze der Verarbeitung personenbezogener Daten Standard?	› Jede Verarbeitung personenbezogener Daten muss die Grundsätze aus Art. 5 Abs. 1 DSGVO einhalten. › Schauen Sie, inwieweit die Prüfung der Grundsätze bzw. der daraus abgeleiteten Anforderungen aus der DSGVO in Regelungen und Prozessen verpflichtend ist.	☐ Ja ☐ Nein
Inwieweit wird „Data protection by design and default” umgesetzt?	› Damit Datenschutz von Anfang an mitgedacht und schon bei der Gestaltung berücksichtigt wird, müssen die Vorgaben aus Art. 25 DSGVO beachtet werden. › Schauen Sie sich an, inwieweit Leitfäden oder Vorgaben für Projekte und IT-Vorhaben entsprechende Vorgaben machen. › Meist ist es unerlässlich, dass Sie als Datenschutzbeauftragter schon in der Ideenphase eingebunden werden. Nur so werden Anforderungen frühzeitig bedacht.	☐ Ja ☐ Nein
Sind die nötigen Datenschutz-Folgenabschätzungen durchgeführt?	› Prüfen Sie, welche Regelungen es zu diesem Aspekt gibt und wie das Vorgehen aussieht. › Entscheidend ist nicht nur, dass Folgenabschätzungen durchgeführt werden. Mindestens genauso wichtig ist, dass man Sie zur Beratung hinzuzieht (Art. 35 Abs. 2 DSGVO). Das sollte als klare Anweisung geregelt sein. › Halten Sie im Verzeichnis von Verarbeitungstätigkeiten Ausschau nach relevanten Verarbeitungen und prüfen Sie, ob die Folgenabschätzungen dokumentiert und mit dem nötigen Inhalt (Art. 35 Abs. 7 DSGVO) durchgeführt wurden.	☐ Ja ☐ Nein
Sind Prozesse zur richtigen Reaktion auf Zwischen-, Not- und Katastrophenfälle eingerichtet?	› Um für den Fall der Fälle vorbereitet zu sein, braucht es entsprechende Pläne und Prozesse sowie die erforderlichen qualifizierten Mitarbeiter. › Haben Sie insbesondere ein Auge auf Regelungen und Prozesse mit Bezug zum Datenschutz, beispielsweise zum Vorgehen bei Datenpannen oder bei einem Hackerangriff.	☐ Ja ☐ Nein
Wie werden Betroffenenrechte gemanagt?	› Hier sind klare Vorgaben zum Vorgehen unerlässlich. So sollte es Prozesse zur Bearbeitung an sich sowie speziell z. B. zum Vorgehen bei Auskunft oder Löschung geben. › Schauen Sie, wie es um das Wissen bei besonders relevanten Stellen steht. Das sind vor allem Kollegen, bei denen Betroffenenanfragen eingehen, etwa der Kundenservice oder die Poststelle. › Auch diejenigen, die Betroffenenrechte umsetzen, müssen über alles Relevante Bescheid wissen.	☐ Ja ☐ Nein
Werden Beschäftigte im angemessenen Umfang geschult, qualifiziert und sensibilisiert?	› Generell gilt: Wer Bescheid weiß, macht weniger falsch und erkennt Gefahren, bevor sie zum Problem werden. Also sollte jeder Mitarbeiter über das für seine Aufgabe nötige Datenschutz-Know-how verfügen. › Schauen Sie, inwieweit es ein Schulungs- und Sensibilisierungskonzept gibt. Auch hier sollte sich die Risikoorientierung widerspiegeln. Außerdem ist das Dokumentieren wichtig. › Klären Sie, inwieweit sichergestellt ist, dass es keine „Durchrutscher“ bei den zu sensibilisierenden Mitarbeitern gibt. Auch im Datenschutz gilt: Eine Kette ist nur so stark wie ihr schwächstes Glied.	☐ Ja ☐ Nein
Sind Dienstleister sorgfältig ausgewählt und passen die vereinbarten Schutzmaßnahmen?	› Meist gibt es Festlegungen zur Auswahl von Dienstleistern. Klären Sie, inwieweit hier auch der Datenschutz eine Rolle spielt. Ist das nicht der Fall, muss das Thema Datenschutz integriert oder ein spezifischer Prozess aufgesetzt werden. › Achten Sie darauf, dass etwa im Verzeichnis von Verarbeitungstätigkeiten auch die beauftragten Dienstleister aufgeführt sind. Idealerweise sind die vereinbarten spezifischen Schutzmaßnahmen vermerkt oder verlinkt.	☐ Ja ☐ Nein
Bestehen Aufbewahrungs- und Löschkonzepte?	› Kennzeichnend für den Datenschutz ist, dass personenbezogene Daten nicht für immer und ewig verarbeitet werden dürfen. › Damit der Löschpflicht aus Art. 17 DSGVO nachgekommen wird, müssen Fristen festgelegt und eine Löschung auch tatsächlich umgesetzt werden.	☐ Ja ☐ Nein

Datenschutz positiv vermitteln – so sorgen Sie für die richtige Vermarktung

Datenschutz wird von manchen Menschen eher als lästige Pflicht gesehen und nicht als Chance wahrgenommen. Dabei liegt genau im Datenschutz viel Positives und guter Datenschutz bringt für alle Vorteile, etwa für Unternehmen, Kunden und Beschäftigte. Dass Datenschutz positiv wahrgenommen wird, haben auch Sie in der Hand. Das ist kein Hexenwerk. So können Sie den Datenschutz besser „verkaufen".

Nicht nur wenn Ihr Unternehmen ein neues Produkt auf den Markt bringen will, ist das hier unerlässlich: das Marketing. Nicht anders ist es, wenn Sie das vielleicht bislang eher ungeliebte Thema Datenschutz zu etwas machen wollen, das jeder gut findet und das jeder bereitwillig unterstützt. Beherzigen Sie diese 5 Tipps:

Tipp 1: Setzen Sie auf eine positive Kommunikation

Braucht man Datenschutz wirklich? Bei solch einer Frage muss ein „Na klar" wie aus Pistole geschossen kommen. Doch diese Antwort sollte nicht nur bei Ihnen kommen. Wichtig ist, dass auch andere im Unternehmen und insbesondere die Entscheidungsträger voll und ganz von dieser Antwort überzeugt sind. Dazu trägt auch bei, dass Sie vom Datenschutz ein positives Bild vermitteln. Machen Sie bei jeder Gelegenheit deutlich, dass gelebter Datenschutz

- **Vorteile im Wettbewerb bringt:** Es ist immer gut, sich von der Konkurrenz abzuheben. Auch Datenschutz kann ein entscheidender Faktor sein.
- **kosteneffizient ist:** Durch gelebten Datenschutz werden Kosten für Schäden und Bußgelder vermieden. Das Geld ist anderswo besser investiert.
- **Vertrauen und Wertschätzung vermittelt:** Kunden und Mitarbeiter wollen, dass ihre Interessen und ihre persönlichen Informationen geschützt sind.
- **die Professionalität Ihres Unternehmens unterstreicht:** Schlampt Ihr Unternehmen im Datenschutz, kann das andere Unternehmen abschrecken.

Tipp 2: Schaffen Sie positive Emotionen

Das Thema Datenschutz muss positive Emotionen auslösen, dass es sich dabei um etwas Gutes und Erstrebenswertes handelt. Das schaffen Sie beispielsweise dadurch, dass Sie bei jeder Gelegenheit Folgendes machen:

- **Betonen Sie immer die Vorzüge:** Werden Sie nicht müde herauszustellen, was Datenschutz bewirkt und welche Benefits er mit sich bringt.
- **Zeigen Sie im Einzelfall die konkreten Vorteile auf:** Das große Bild vermitteln ist eine Sache. Viel greifbarer wird manches, wenn Sie etwa bei einem Vorhaben die Vorzüge konkret benennen.
- **Setzen Sie auf den Dominoeffekt:** Egal, ob Projekt oder Menschen, hat man mit Ihnen, Ihrer Arbeit oder dem Datenschutz positive Erfahrungen gemacht, wird man das Positive gern weitergeben. Mundpropaganda funktioniert noch immer ausgezeichnet und ohne dass Sie diese aktiv steuern müssen.

Tipp 3: Entwickeln Sie eine umfassende Kommunikationsstrategie

Ihr Ziel ist, dass Datenschutz präsenter und positiver wahrgenommen wird. Um das zu erreichen, ist eine gute Kommunikationsstrategie unerlässlich. Am besten ist es, wenn Sie sich hier mit den Kommunikationsspezialisten in Ihrem Unternehmen zusammensetzen. Erläutern Sie ganz offen, was Ihr Ziel ist. Die Kollegen können Ihnen nicht nur Strategietipps an sich geben. Sie haben auch einen guten Blick dafür, wie Sie Ihr Thema erfolgreich transportieren können bzw. wie Sie die Beschäftigten am besten erreichen. Auch sind die Kollegen meist die Türöffner schlechthin, wenn es um die Nutzung von Intranet, Mitarbeiterzeitung oder internem E-Mail-Newsletter geht. Etwa ein „Datenschutz-Tipp des Monats" kann eine gute Möglichkeit sein, Datenschutz kurzweilig näherzubringen.

Aber Vorsicht: Achten Sie bei einer solchen Strategie auch auf die Machbarkeit. Haben Sie kaum Zeit? Oder ist Texten bzw. interessante Artikel schreiben nicht Ihr Ding? Dann brauchen Sie jemanden, der das für Sie übernehmen kann. Eventuell sind in einem solchen Fall andere Formen der Kommunikation besser für Sie. So z. B. kurze Schulungen, die Sie rund um die Mittagspause anbieten. Auch eine offene Sprechstunde ist eine Möglichkeit.

Tipp 4: Setzen Sie Erfolge ins rechte Licht

Wann haben Sie zuletzt über Positives rund um den Datenschutz in Ihrem Unternehmen informiert? Wenn Sie sich nicht mehr daran erinnern können, heißt es, die Ärmel hochkrempeln. Ändern Sie das schleunigst. Schließlich tragen Sie als Datenschutzbeauftragter entscheidend dazu bei, dass es diese Erfolge gibt. Feiern Sie Erfolge und berichten Sie anlassbezogen. Ansonsten bekommt das Management überhaupt nicht mit, dass gemeinsam mit dem ausländischen Dienstleister nach zähen Verhandlungen endlich das Thema Auftragsverarbeitung abgehakt werden kann. Im Übrigen sollten Sie Erfolgsberichte zum regelmäßigen Bestandteil Ihrer Rücksprachen machen. Dabei müssen Sie sich nicht selbst loben. Erwähnen Sie einfach, dass Sie stolz auf das Erreichte sind.

Tipp 5: Sparen Sie nicht mit Lob

Lob weiß jeder zu schätzen. Dabei ist ein Lob nicht nur Wertschätzung. Es ist Antrieb für weitere Unterstützung und zugleich Motivation für andere. Ist etwas richtig gut gelaufen oder hat man Sie tatkräftig unterstützt, sollten Sie Ihr Lob nicht nur gegenüber den betreffenden Personen aussprechen. Platzieren Sie Ihr Lob auch anderswo, etwa an höherer Stelle. Das wirkt dann besonders nachhaltig.

Personelle Änderungsmitteilungen: Diese Aspekte sollten Sie prüfen

In jedem Unternehmen gibt es personelle Veränderungen. Da kommen neue Mitarbeiter ins Unternehmen, andere verlassen es und wiederum andere wechseln die Aufgabe oder die Abteilung. Damit das Unternehmen weiter gut funktioniert, muss über solche Veränderungen informiert werden. Was nach einer einfachen Sache klingt, ist bei genauerem Hinsehen von großer Datenschutzrelevanz. Machen Sie den Check, ob alles in Ordnung ist!

Information über Veränderungen sind unerlässlich

Dass über Veränderungen informiert wird, liegt nicht nur im Interesse des Unternehmens, den Betrieb und die Geschäftstätigkeit gut zu organisieren. Solche Mitteilungen sind auch ansonsten sehr wichtig. So wird etwa bekannt, wer zukünftig welche Aufgabe wahrnimmt. Damit können andere Zuständigkeiten und Verantwortlichkeiten einhergehen. Auch ist die Information wichtig, um etwa die Berechtigung einer Person leicht nachvollziehbar zu kommunizieren. Wechselt ein Mitarbeiter von Abteilung A zu Abteilung B und nimmt er eine andere Aufgabe wahr, braucht er zukünftig nicht mehr wissen, was in Abteilung A läuft. Entsprechend benötigt er auch keinen Zugriff mehr auf (personenbezogene) Daten der Abteilung A.

Dass Informationen über personelle Veränderungen wichtig sind, wird erst recht deutlich, wenn Mitarbeiter das Unternehmen verlassen, vielleicht nicht wirklich im Guten. Dann ist es für die Mitarbeiter unerlässlich zu wissen, dass Herr X ab dem kommenden Monat nicht mehr im Unternehmen ist. Das kann beispielsweise schon im Vorfeld bei der Weitergabe von Informationen bedacht werden, damit ein Datenfluss gestoppt wird.

Informationen sind wichtig für den Datenschutz
Bedenken Sie als Datenschutzbeauftragter stets: Änderungsmitteilungen sind eine organisatorische Maßnahme, um die Umsetzung der Anforderungen aus der Datenschutz-Grundverordnung (DSGVO) sicherzustellen. Eine solche Information trägt dazu bei, Art. 24 Abs. 1 bzw. Art. 32 DSGVO umzusetzen. Denn: Zwar gibt es vielleicht Standardprozesse, die etwa den Entzug von Berechtigungen beim Abteilungswechsel oder beim Austritt aus dem Unternehmen sicherstellen. Manches läuft aber auch ohne Prozesse. Wissen Mitarbeiter, wer zukünftig nicht mehr „befugt" ist, können sie ihr Handeln entsprechend ausrichten.

CHECKLISTE: Datenschutzaspekte bei personellen Mitteilungen

Aspekt	Darauf sollten Sie achten	Geprüft?
Über wen soll konkret informiert werden?	› Fragen Sie nach, welche Rolle und Funktion die betreffende Person im Unternehmen haben wird oder bislang hatte. › Auch die hierarchische Einordnung kann relevant sein. Es hat eine andere Bedeutung, ob ein leitender Angestellter oder ein „normaler" Mitarbeiter im Fokus steht. › Machen Sie klar, dass eine individuelle Betrachtung nötig ist. Zudem hängt von der entsprechenden Funktion ab, wie umfangreich ggf. die Information sein kann oder muss.	☐ Ja ☐ Nein
Welchen Anlass gibt es für die Mitteilung?	› Denken Sie hier vor allem an Eintritt, Versetzung bzw. Antritt einer neuen Aufgabe oder Ende der Tätigkeit. › Der Anlass kann ebenfalls von Bedeutung sein, wenn es um die Ausführlichkeit der Information geht. › Manchmal muss auch mitgeteilt werden, dass es zur Veränderung aufgrund eines Todesfalls kommt. Dabei ist klar: Für den Verstorbenen gilt die DSGVO nicht mehr. Diese greift nur für lebende natürliche Personen. Insofern kann hier leichter über eine Veränderung berichtet werden. Allerdings sollte eine Information dennoch dem Anspruch an Anstand und Würde genügen. Also verbieten sich etwa Informationen zur Todesursache.	☐ Ja ☐ Nein
Welche Informationen sollen gegeben werden?	› Hier heißt es, genau hinschauen. Unter Umständen können auf den ersten Blick weniger relevante Informationen zum Problem werden. So z. B. zum Grund der Veränderung oder zum „Vorleben" eines neuen Mitarbeiters. › Bestehen Sie auf einer konkreten Auflistung der relevanten Informationen. › Lassen Sie sich nach Möglichkeit einen Entwurf zur Prüfung und Bewertung vorlegen. Manche Formulierungen sind problematisch, auch wenn sie belanglos wirken. So z. B. „Herr X verlässt uns, weil er bei der Firma Y das Marketing übernimmt".	☐ Ja ☐ Nein
Woher stammen die betreffenden Informationen?	› Diese Frage sollte nicht unterschätzt werden. Vielleicht hat man manches über einen neuen Mitarbeiter über eine Suchmaschine oder ein soziales Netzwerk gefunden. Doch nur weil man es findet, darf es noch lange nicht verwendet werden. Das gilt gerade auch für soziale Netzwerke oder Veröffentlichungen auf Webseiten oder in Foren. › Klären Sie auch, wer welche Daten zur Verfügung gestellt hat bzw. von wem die Daten beschafft wurden. Denn schon für das Beschaffen bedarf es regelmäßig einer Rechtsgrundlage.	☐ Ja ☐ Nein

CHECKLISTE: Datenschutzaspekte bei personellen Mitteilungen		
Werden nur dienstlich relevante Informationen mitgeteilt?	› In personellen Veränderungsmitteilungen werden oft dienstliche und private Informationen vermischt. Dabei gilt: Allenfalls was dienstlich relevant ist, kann wirklich erheblich sein. › Privates oder nicht für die konkrete Mitteilungssituation relevante Informationen sind prinzipiell tabu (z. B. Geburtsdatum, Alter, Geburtsname, familiäre Situation, Hobbys, früherer Arbeitgeber). Hierfür wird es meist keine Rechtsgrundlage außer der Einwilligung des Betroffenen geben. Und bei der müssen viele Besonderheiten beachtet werden, gerade bei Beschäftigten. › Hinterfragen Sie auch bei eher dienstlichen Informationen die Notwendigkeit. Nur weil etwas für die Empfänger interessant ist, ist das noch lange nicht ausreichend, um eine Veröffentlichung aller dienstlichen Informationen zu rechtfertigen.	☐ Ja ☐ Nein
Inwieweit soll ein Foto in die Mitteilung aufgenommen werden?	› Ein Foto ist regelmäßig nicht für die Information über personelle Veränderungen erforderlich. Das wird man nicht auf § 26 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG, Durchführung eines Beschäftigungsverhältnisses) bzw. auf Art. 6 Abs. 1 Satz 1 Buchst. b DSGVO (Vertragserfüllung) stützen können. Es bleibt für ein Foto nur die Einwilligung des betreffenden Beschäftigten. › Bei Verstorbenen sind zwar personenbezogene Daten meist unproblematisch, weil die DSGVO nicht mehr gilt. Bei Fotos ist Vorsicht angebracht. Nach § 22 Satz 3 Kunsturhebergesetz bedarf es bis zum Ablauf von 10 Jahren der Einwilligung der Angehörigen des Abgebildeten.	☐ Ja ☐ Nein
Auf welche Rechtsgrundlage soll die Mitteilung gestützt werden?	› Beachten Sie stets: Jede enthaltene Information bedarf einer Rechtsgrundlage. Schließlich ist jede enthaltene Information auf eine natürliche Person bezogen, eben denjenigen, um den es in der Mitteilung geht. › Für Beschäftigte kommt § 26 Abs. 1 BDSG in Betracht, etwa zur Durchführung bei Aufnahme oder Wechsel einer Tätigkeit im Unternehmen. › Bei der Beendigung eines Beschäftigungsverhältnisses wird es jedoch meist an der Erforderlichkeit für diese Information fehlen, sodass § 26 Abs. 1 Satz 1 BDSG nicht passt. Daher müssen alternative Rechtsgrundlagen geprüft werden. So z. B. das überwiegende berechtigte Interesse (Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO). Allerdings dürfen hierbei die Interessen oder Grundrechte und Grundfreiheiten des Betroffenen nicht überwiegen. Das ist bei nicht dienstlich relevanten Informationen aber der Fall. Bedenken Sie stets, dass der Begriff des Beschäftigten sehr weit reicht (§ 26 Abs. 8 BDSG). Umfasst sind auch Bewerber, Azubis oder frühere Mitarbeiter.	☐ Ja ☐ Nein
Bei Einwilligungen: Sind alle Anforderungen eingehalten?	› Will Ihr Unternehmen auf die Einwilligung setzen, greifen die Besonderheiten für Beschäftigte nach § 26 Abs. 2 BDSG. › Gerade die Freiwilligkeit kann hier problematisch sein, etwa bei neuen oder ausscheidenden Mitarbeitern. Wegen des Abhängigkeitsverhältnisses muss besonders auf eine freie Wahlmöglichkeit für den Betroffenen geachtet werden. › Zwar muss eine Einwilligung nicht zwingend in Schriftform erklärt werden. Allerdings muss Ihr Unternehmen die Einwilligung im Zweifel auch nachweisen können. Kann es das nicht, liegt keine Rechtsgrundlage vor.	☐ Ja ☐ Nein
Wie und wo soll die Information erfolgen?	› In Betracht kommt beispielsweise eine Mitteilung per E-Mail oder auch eine Veröffentlichung im Intranet. Das hat erhebliche Auswirkungen auf die Reichweite der Informationen. › Soll es sogar eine Veröffentlichung auf der Webseite geben oder sollen andere Unternehmen informiert werden, muss genauer hingeschaut werden. Manche Informationen, die bei einer internen Veröffentlichung in Ordnung sind, dürfen gegenüber Dritten nicht gegeben werden. Bedenken Sie auch hier stets das Minimalprinzip und damit die Faustformel „Kenntnis nur, wenn erforderlich“.	☐ Ja ☐ Nein
Welcher Empfängerkreis soll die Informationen erhalten?	› Nicht jede personelle Veränderung ist für jeden im Unternehmen von Relevanz. Auch bezüglich des Empfängerkreises sollte das Minimalprinzip umgesetzt werden. › Gerade bei einer Meldung zu einem Beschäftigungsende gilt: Orientieren Sie sich einerseits an der Funktion und Bedeutung der betreffenden Person. Andererseits können auch die hierarchische Einordnung bzw. die disziplinarischen Befugnisse erheblich sein. Es macht einen großen Unterschied, ob es um jemanden in der Führung oder einen Mitarbeiter ohne Entscheidungsbefugnisse geht.	☐ Ja ☐ Nein
Wird der Grundsatz der Datenminimierung insgesamt eingehalten?	› Bei einem Entwurf sollten Sie bzw. die Kollegen vor einer Veröffentlichung noch einmal einen ganzheitlichen Check machen, und zwar insbesondere hinsichtlich der Aspekte Erforderlichkeit und Datenminimierung. Fehlt es an der Notwendigkeit der Information bzw. einzelner Bestandteile, sollte eine Veröffentlichung entsprechend unterbleiben. › Empfehlen Sie, dass jemand gegenliest, der mit der Erstellung nichts zu tun hatte, etwa ein anderer Kollege aus der Personalabteilung. Dieser sollte vor allem auf den Aspekt der Erforderlichkeit einzelner Informationen achten.	☐ Ja ☐ Nein

Zutrittskontrolle: Haben Sie ein Auge auf diese Schwachstellen

In jedem Unternehmen gibt es sie in irgendeiner Form. Egal ob mit Schlüssel, Chipkarte, Dongle oder Fingerabdruck, der Zutritt zum Unternehmen wird immer auf die eine oder andere Weise beschränkt. Dabei liegt auf der Hand: Es sind eigentlich immer personenbezogene Daten im Spiel. Also sollten Sie die Sache einmal genauer unter die Lupe nehmen.

Prüfen Sie im Gespräch

Wie bei jeder Verarbeitung personenbezogener Daten, gibt es auch bei der Zutrittssteuerung bzw. Zutrittskontrolle typische Schwachstellen, bei denen Sie genauer hinschauen sollten. Setzen Sie sich mit den zuständigen Kollegen zusammen und arbeiten Sie die folgende Checkliste durch. Stellen Sie fest, dass es an einer Stelle nicht passt, sollte das entsprechend zeitnah angegangen werden. Schließlich gilt: Defizite erkennen ist nicht schlecht, Defizite beheben ist aber erst gut.

CHECKLISTE: Typische Schwachstellen bei der Zutrittskontrolle

Aspekt	Darauf sollten Sie achten	Geprüft?
Fehlendes Gesamtkonzept	› Die Zutrittskontrolle ist ein Baustein in einem Gesamtkonzept zur Absicherung des Unternehmens. Lassen Sie sich dieses Gesamtkonzept vorlegen und schauen Sie, inwieweit dieses Hand und Fuß hat. Die Maßnahmen sollten zueinander passen und am besten miteinander verzahnt sein. › Klären Sie, inwieweit Zuständigkeiten und Verantwortlichkeiten klar definiert sind. › Achten Sie auch auf Regelungen. Ohne Regelungen und Vorgaben wird vieles mal so und mal so gehandhabt.	☐ Ja ☐ Nein
Lückenhafte oder fehlende Datenschutzdokumentation	› Klären Sie, inwieweit alle datenschutzrelevanten Aspekte geprüft und dokumentiert sind. Gibt es Lücken, sollten diese geschlossen werden. › Werfen Sie einen Blick ins Verzeichnis von Verarbeitungstätigkeiten. Die Angaben müssen vollständig und aktuell sein.	☐ Ja ☐ Nein
Defizite bei der Berechtigungsvergabe	› Hinterfragen Sie das Thema Berechtigungen und Berechtigungskonzept insgesamt. Lassen Sie sich erklären, wie dieses aufgebaut ist. › Schauen Sie sich die Prozesse zur Vergabe von Berechtigungen an. Hier sollte es klare Standards und keine Vergabe „auf Zuruf“ geben. › Prüfen Sie, wie Berechtigungen bei Besuchern gemanagt werden.	☐ Ja ☐ Nein
Zu weitreichende Berechtigungen	› Meist ist es sinnvoll, Rollen zu definieren, die über bestimmte Zutrittsberechtigungen verfügen, etwa funktions- oder aufgabenbezogen. Diesen Rollen werden die einzelnen Mitarbeiter zugeordnet. › Achten Sie darauf, inwieweit bei Berechtigungen das Minimalprinzip umgesetzt ist. Grundsätzlich gilt: Zutritt nur, wenn für die Aufgabe oder Funktion erforderlich.	☐ Ja ☐ Nein
Fehlender zeitnaher Berechtigungsentzug	› Idealerweise gibt es hier einen Automatismus, der etwa von der Fachabteilung oder der Personalabteilung gestartet wird. › Auf jeden Fall müssen Berechtigungen unverzüglich entzogen werden, wenn ein Mitarbeiter das Unternehmen verlässt. Auch bei einem Aufgabenwechsel ist eine schnelle Anpassung nötig.	☐ Ja ☐ Nein
Datenschutzrechtlich unzulässige biometrische Verfahren	› Meist wird eine biometrische Zutrittskontrolle (z. B. mittels Fingerabdrucks) im datenschutzrechtlichen Sinn nicht erforderlich sein. Es gibt mildere Mittel mit weniger sensiblen Daten, etwa Chipkarte oder Dongle. › Oft bleibt nur die Einwilligung als Rechtsgrundlage. Die ist gerade im Beschäftigungsverhältnis problematisch. Die Anforderungen sind hoch (§ 26 Abs. 2 Bundesdatenschutzgesetz).	☐ Ja ☐ Nein
Mangelhafte Datensicherheit	› Einerseits handelt es sich um eine sicherheitsrelevante Einrichtung selbst, andererseits werden damit personenbezogene Daten verarbeitet. Es muss also Art. 32 Datenschutz-Grundverordnung (DSGVO) umgesetzt sein, sprich, es muss risikoangemessene Schutzmaßnahmen geben. › Hinterfragen Sie, inwieweit die Schutzmaßnahmen tatsächlich passen. Gerne wird hier auf ein „Hochglanzprospekt“ des Anbieters verwiesen. Das orientiert sich aber nicht an den konkreten Risiken Ihres Unternehmens.	☐ Ja ☐ Nein
Fehlende Datenschutzvereinbarungen	› Eventuell wird ein System genutzt, das über ein Portal des Anbieters gesteuert oder verwaltet wird. Hier liegt oft ein Fall der Auftragsverarbeitung (Art. 28 DSGVO) vor. › Prüfen Sie, inwieweit es eine entsprechende Vereinbarung gibt und ob Schutzmaßnahmen festgelegt bzw. umgesetzt sind.	☐ Ja ☐ Nein
Zweckwidrige Verwendung von Daten	› Daten, die für einen bestimmten Zweck verarbeitet werden, dürfen nicht einfach für einen anderen Zweck verwendet werden. Hier muss Art. 6 Abs. 4 DSGVO beachtet werden. › Betriebsvereinbarungen können Verwendungsverbote enthalten. Dann kann eine Verarbeitung für einen anderen Zweck ausscheiden.	☐ Ja ☐ Nein

Nicht im Urlaub erreichbar: Droht mir Ärger?

FRAGE: Ich bin Datenschutzbeauftragter und nehme die Funktion nebenbei wahr. Während meines dreiwöchigen Urlaubs kam es zu einem Hackerangriff. Bei dem wurden Daten gestohlen. Gegenmaßnahmen wurden ergriffen. Was aber wohl nicht passiert ist, ist die Meldung dieser Datenpanne an die Datenschutzaufsichtsbehörde. Nach meinem Urlaub hatte ich ein Gespräch mit einem verärgerten Geschäftsführer. Der meinte, dass die vergessene Meldung meine Schuld wäre. Es könne nicht sein, dass ich während des Urlaubs nicht erreichbar wäre. Er meinte, dass er mir nun die Weisung erteile, vor dem nächsten Urlaub Kontaktdaten zu hinterlegen, damit ich für den Fall der Fälle erreichbar bin. Meine Frage daher: Muss ich das mit mir machen lassen? Kann mir arbeitsrechtlicher Ärger drohen, weil ich im letzten Urlaub nicht erreichbar war?

ANTWORT: Zunächst einmal zum letzten Urlaub. Arbeitsrechtlicher Ärger, etwa eine arbeitgeberseitige Abmahnung, dürfte nicht drohen. Hier fehlt jeder Grund, weil Ihnen kein Verstoß gegen den Arbeitsvertrag oder Ihre Pflichten als Arbeitnehmer vorzuwerfen ist. Sie waren in Urlaub und das war und ist Ihr gutes Recht. Dabei ist wichtig: Der Zweck des Urlaubs ist Erholung. Dementsprechend spricht auch der Gesetzgeber im Bundesurlaubsgesetz von Erholungsurlaub (§ 1 BUrlG). Außerdem sieht § 8 BUrlG vor, dass Sie während des Urlaubs keiner Erwerbstätigkeit nachgehen dürfen, die dem Urlaubszweck widerspricht. Sollte es dennoch zu einer Abmahnung kommen, heißt es handeln. Diese sollten Sie nicht hinnehmen. Vielmehr sollten Sie mithilfe des Betriebsrats bzw. eines Anwalts dagegen vorgehen. Schließlich wäre sie haltlos.

Sie dürfen nicht erreichbar sein

Generell sollten Sie hinsichtlich einer „Mitteilungspflicht von Kontaktdaten" eines wissen: Eine solche Pflicht besteht nicht. Denn es gilt Folgendes:

- Die Datenschutz-Grundverordnung (DSGVO) sieht nicht vor, dass Sie als Datenschutzbeauftragter immer erreichbar sein müssen, etwa um bei Fragen zum Datenschutz zur Verfügung zu stehen. Das gilt auch für Fragen oder eine Beratung im Zusammenhang mit einem Hackerangriff oder sonstigen Datenpannen.
- Die Anforderungen der DSGVO richten sich an den Verantwortlichen. Er muss die nötigen Maßnahmen ergreifen, um die DSGVO umzusetzen. Braucht er hierfür Beratung, muss er sicherstellen, dass diese jederzeit verfügbar ist. Und hier gibt es einige Möglichkeiten: So kann er einen Stellvertreter für Sie benennen. Daneben kann jedoch auch auf externe Beratungslösungen zurückgegriffen werden. So kann im Fall der Fälle ein externer Datenschutzberater unterstützen oder eben auch ein Anwalt.
- Einfach zu sagen, dass man wegen Ihres Urlaubs nicht eine Meldung durchführen konnte, ist zumindest unfair. Schließlich trifft die Pflicht den Verantwortlichen und in letzter Konsequenz die Unternehmensleitung. Diese muss ihre Geschäfte so führen, dass es zu keinen Gesetzesverstößen kommt. Kann sie das nicht selbst beurteilen, muss sie für Rat sorgen.
- Für Sie besteht keine Verpflichtung mitzuteilen, wo Sie Urlaub machen oder wie man Sie im Urlaub erreichen kann. Das lässt sich einerseits arbeitsrechtlich nicht begründen. Andererseits ist es auch datenschutzrechtlich nicht drin. So lässt sich die Verarbeitung der betreffenden Kontaktinformationen nicht auf § 26 Abs. 1 Satz 1 Bundesdatenschutzgesetz bzw. auf Art. 6 Abs. 1 Satz 1 Buchst. b DSGVO stützen. Die Informationen sind für die Durchführung des Beschäftigungsverhältnisses bzw. eines Vertrags mit dem Betroffenen nicht erforderlich. Ein überwiegendes berechtigtes Interesse scheidet aus, weil schon wegen der gesetzgeberischen Wertungen zum Urlaubszweck Ihre Interessen überwiegen dürften. Verbleibt also nur Ihre Einwilligung. Und an die werden hohe Anforderungen gestellt (§ 26 Abs. 2 DSGVO), etwa dass Sie die freie Entscheidung haben, ob Sie Daten zur Verfügung stellen oder nicht.

Suchen Sie das klärende Gespräch

Meist ist es besser, in einem Gespräch nach einer Lösung zu suchen, die allen Interessen gerecht wird. Das dürfte im Fall der Fälle ein externer Datenschutzberater sein, der eingebunden werden kann, wenn es wirklich brennt.

§ 26 BDSG ungültig? Müssen wir die Verarbeitungen umstellen?

FRAGE: Ich habe gehört, dass § 26 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) nach einem Urteil des Europäischen Gerichtshofs (EuGH) für Verarbeitungen im Beschäftigungskontext nicht mehr anwendbar sein soll. Müssen wir nun entsprechende Verarbeitungen auf Art. 6 Abs. 1 Satz 1 Buchst. b Datenschutz-Grundverordnung (DSGVO, Vertrag) umstellen?

ANTWORT: Die Sache ist umstritten. Zurück geht die Diskussion auf ein Urteil des EuGH vom 30.3.2023 (Rs. C-34/21). Dort hat der EuGH entschieden, dass er eine vergleichbare Regelung im Hessischen Datenschutz- und Informationsfreiheitsgesetz für nicht mit der DSGVO vereinbar hält. Allerdings: Der EuGH antwortete in diesem Verfahren nur auf die vorgelegten Fragen. Nach § 26 BDSG wurde nicht gefragt und daher auch nichts dazu entschieden. Insofern sind manche der Ansicht, dass § 26 Abs. 1 Satz 1 BDSG weiterhin anwendbar ist. Wollen Sie jedoch auf Nummer sicher gehen, kann es sinnvoll sein, die Rechtsgrundlage auf Art. 6 Abs. 1 Satz 1 Buchst. b DSGVO abzuändern.

LAG: Arbeitgeber darf mit Befragungen Pflichtverletzung aufklären

Auch wenn Arbeitgeber ihren Beschäftigten manches erlauben, etwa Räume oder Werkzeuge für private Zwecke zu nutzen, heißt das nicht, dass es nicht doch schwarze Schafe geben kann. Und die übertreiben es dann mit dem Erlaubten. So war es auch in einem Fall, den das Landesarbeitsgericht (LAG) Niedersachsen zu entscheiden hatte (Urteil vom 15.1.2025, Az. 2 SLa 31/24).

Diese Sache landete vor Gericht

Eine Firma, die spätere Beklagte, beschäftigte einen Mann als Schichtführer, den späteren Kläger. Dieser war Vorgesetzter für mehrere Mitarbeiter in der Produktion. Bis zum November 2022 gab es für Mitarbeiter die Möglichkeit, beispielsweise nicht mehr benötigtes Material für private Zwecke mitzunehmen. Dazu bedurfte es eines Freigabescheins. Diese Erlaubnis wurde widerrufen. Auf Nachfrage des Mannes bestätigte der Produktionsleiter im Februar 2023 nochmals, dass dies nicht mehr möglich ist. Der Mann besorgte über einen Mitarbeiter einen Blanko-Freigabeschein. Unter dem Vorwand, am Samstag, dem 1.4.2023, Schränke aus der Produktion verladen zu wollen, holte der Mann jedoch Kanthölzer ab.

Mitarbeiter melden die Sache

Das Verladen der Kanthölzer blieb nicht unbemerkt. Mehrere Mitarbeiter spielten dem Betriebsrat anonym Videos zu. Bei der Befragung durch den Betriebsratsvorsitzenden und einen Mitarbeiter der Personalabteilung äußerte der Mann, dass alles in Ordnung wäre. In den folgenden Tagen wurden jedoch von Mitarbeitern weitere Vorfälle gemeldet. So z. B., dass der Mann Mitarbeiter gedrängt hatte, Gegenstände für seinen privaten Gebrauch zu bauen. Einen anderen Mitarbeiter wies er an, die Sägeketten der privaten Motorsäge zu schärfen, und wiederum einen anderen Mitarbeiter, Platten wohl für die private Verwendung zu schneiden.

Unternehmen klärt die Sache auf

Dazu wurden mit einem umfangreichen Fragenkatalog alle Mitarbeiter befragt. Nach Auswertung der Antworten und erfolgter Anhörung kündigte das Unternehmen dem Schichtführer. Der Grund: dringender Verdacht einer schwerwiegenden Pflichtverletzung aufgrund der unerlaubten Mitnahme von Kanthölzern sowie die Anweisung der Erledigung privater Arbeiten durch andere Mitarbeiter. Gegen diese Kündigung klagte der Mann vor dem Arbeitsgericht. Allerdings ohne Erfolg. Also versuchte der Mann, das LAG davon zu überzeugen, dass die Kündigung unzulässig war, etwa weil er durch die Befragung aller Mitarbeiter in seinem Persönlichkeitsrecht verletzt wurde. Doch auch das LAG ließ sich von dieser Argumentation nicht überzeugen.

So urteilte das LAG

Die außerordentliche Kündigung durch das Unternehmen ist nicht zu beanstanden. Eine außerordentliche Kündigung ist zulässig, wenn ein wichtiger Grund im Sinne von § 626 Bürgerliches Gesetzbuch (BGB) vorliegt. Dabei kann auch der Verdacht einer schwerwiegenden Pflichtverletzung einen wichtigen Grund darstellen, wenn objektiv gesehen die Verdachtsmomente das für ein Arbeitsverhältnis erforderliche Vertrauen zerstören.

Es muss nicht zwangsläufig gegen arbeitsvertragliche Hauptpflichten verstoßen werden. Auch der Verstoß gegen Nebenpflichten reicht aus, etwa die Pflicht zur Rücksichtnahme auf die Interessen und Rechtsgüter der anderen Partei. Dass der Schichtführer Mitarbeiter anwies, für ihn private Arbeiten während der Arbeitszeit mit Betriebsmitteln durchzuführen, stellt ein Ausnutzen seiner Vorgesetztenfunktion dar. Dies erschüttert die Integrität des Schichtführers so sehr, dass ein wichtiger Grund anzunehmen ist.

Erkenntnisse durften verwendet werden

Bezüglich der Aussagen aus der durchgeführten Befragung der Mitarbeiter besteht kein Beweisverwertungsverbot. Insbesondere ist kein Verstoß gegen § 26 Abs. 1 Satz 2 Bundesdatenschutzgesetz (BDSG) zu erkennen. Gerade vor Ausspruch einer außerordentlichen Kündigung ist es erforderlich, den Sachverhalt gründlich und erschöpfend aufzuklären. Doch selbst wenn man einen Verstoß gegen § 26 Abs. 1 Satz 2 BDSG annimmt, besteht kein Verwertungsverbot. Die Verwertung der Erkenntnisse führt zu keinem Grundrechtsverstoß. Die Handlungen des Mannes geschahen in der Betriebsöffentlichkeit. Insofern musste er damit rechnen, dass die Pflichtverletzungen auch durch Befragungen aufgedeckt und verfolgt würden. Eine heimliche Überwachung hat nicht stattgefunden.

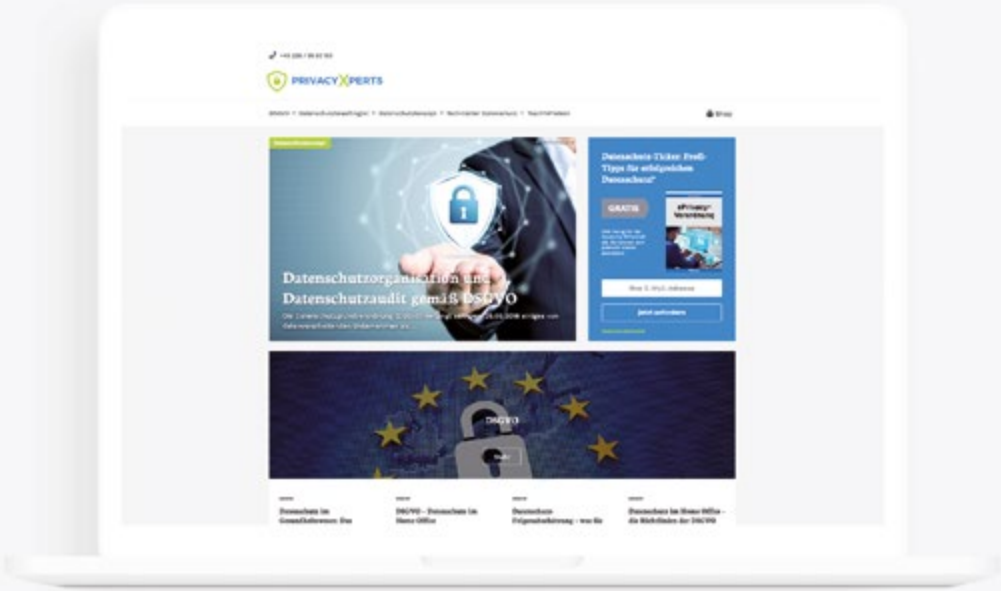
Kein Mitbestimmungsrecht verletzt

Ein Beweisverwertungsverbot ergibt sich auch nicht daraus, dass Fragebögen mitbestimmungspflichtig sein können. Sachbezogene Fragen, etwa zur Aufklärung von Straftaten, sind auch dann nicht von § 94 Abs. 1 Betriebsverfassungsgesetz (BetrVG) erfasst, wenn keine Anonymität gegeben und die Beantwortung für die Mitarbeiter verpflichtend ist. Auch ist mit der Befragung insbesondere nicht gegen die Grundsätze von Recht und Billigkeit (§ 75 BetrVG) und Treu und Glauben (§ 242 BGB) verstoßen worden.

Das können Sie aus dem Urteil folgern

Es gibt kein Recht auf heimliche Begehung einer Pflichtverletzung. Hier hilft es der betreffenden Person auch nicht, mit dem Datenschutz oder Persönlichkeitsrecht zur argumentieren. Auch besteht bei einem Datenschutzverstoß nicht automatisch ein Verwertungsverbot, sodass eine Kündigung unwirksam wäre. Erinnern Sie sich an das Urteil, wenn Sie zum Vorgehen bei Pflichtverletzungen beraten sollen.

„Datenschutz aktuell“ ist ein Produkt der PrivacyXperts-Familie!



Als Fachverlag für Beratung im Bereich Datenschutz und IT-Security sind Sie bei uns genau an der richtigen Adresse, wenn es um Ihre Themen geht. Lassen Sie sich über unsere Fachinformationsdienste und Portale rund um neue EU-Verordnungen, aktuelle Urteile zum Datenschutzrecht oder über die umfangreichen Dokumentationspflichten für Datenschutzverantwortliche informieren. So erhalten Sie nützliche Informationen und Praxistipps für Ihre Arbeit und sind beim Thema Datenschutz bestens aufgestellt.

Stellen Sie eine direkte Verbindung zu verlässlichen Informationen und aktuellen Entwicklungen her und entdecken Sie viele weitere Datenschutz-Produkte unter www.privacyxperts.de/shop

Schnell und effektiv Mitarbeiter schulen!

Jetzt Mitarbeiterinformation bestellen

https://t1p.de/gmxhs

Vorschau:

NIS-2-Richtlinie: So gehen Sie damit um
Fehler sind gut: Fördern Sie die Fehlerkultur

PRIVACYXPERTS

Telefon: 02 28 95 50 150
Fax: 02 28 36 96 480
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de

Ein Unternehmensbereich des VNR Verlags
für die Deutsche Wirtschaft AG
Theodor-Heuss-Straße 2–4
53177 Bonn